JOURNAL OF NUMBER THEORY 13, 66–87 (1981)

Ein Reziprozitätsgesetz in Galoisfeldern

KLAUS BURDE

Institut D für Math d. TU, Braunschweig, Pockelsstrasse 14, 33 Braunschweig, West Germany

Communicated by H. Zassenhaus

Received July 26, 1979

In einer früheren Arbeit [K. Burde, *J. Reine Angew. Math.* **293/294** (1977), 418] formulierte ich Reziprozitätsgesetze für kubische und biquadratische Reste als Beziehungen in einem Restklassenkörper $\mathbb{Z}_p$ und leitete aus diesen entsprechende komplexe und rationale Reziprozitätsgesetze ab. Die dortigen Ergebnisse werden hier in zweierlei Hinsicht verallgemeinert. Zum einen werden jetzt beliebige n-te Potenzreste betrachtet, zum andern wird der Restklassenkörper $\mathbb{Z}_p = GF(p)$ durch ein beliebiges Galoisfeld $GF(p^f)$ ersetzt. Letzteres gestattet— in der komplexen Anwendung—die Behandlung der komplexen Reziprozitätsgesetze auch in den Fällen, in denen Primideale eines Grades $f > 1$ auftreten. In §1 wird ein "Reziprozitätsgesetz für n-te Potenzreste in Galoisfeldern" aufgestellt. Aus diesem werden in §2 komplexe und in §3 rationale Reziprozitätsgesetze gewonnen. Einige, für das Verständnis nicht wesentliche Beweise sind in einem Anhang zusammengestellt, auf den mit—(A.∗)—verwiesen wird.

1. Ein Reziprozitätsgesetz in Galoisfeldern

Es sei $n > 1$ eine natürliche Zahl, p eine n nicht teilende rationale Primzahl und $f \in \mathbb{N}$ ein "zu n und p gehöriger Exponent," d.h. es gelte

$$p^f \equiv 1(n), \qquad 1 < n \in \mathbb{N}. \tag{1.1}$$

Das Galoisfeld $GF(p^f)$ enthalte also die n-ten Einheitswurzeln bzw. den n-ten Kreiskörper über $\mathbb{Z}_p = GF(p)$.

Wir erklären den "Eulercharakter modulo p^f der Ordnung n" durch

$$\chi_{p^f,n} = \chi: \quad \chi(a) = \left(\frac{a}{p^f}\right)_n = a^{(p^f-1)/n} \in GF(p^f); \qquad a \in GF(p^f). \tag{1.2}$$

Seine Werte, die "n-ten Potenzrestsymbole modulo p^f," sind n-te Einheitswurzeln aus $GF(p^f)$.

Ist $\sigma_p: x \mapsto x^p$; $x \in GF(p^t)$ der kanonische erzeugende Automorphismus

0022-314X/81/010066–22$02.00/0

der Galoisgruppe einer Erweiterung $GF(p^t)/\mathbb{Z}_p$, so gilt für jede n-te Wurzel $a^{1/n}$ eines Elementes $a \in GF(p^f)$—in einer Erweiterung $GF(p^t)$—

$$\begin{aligned} \sigma_p^f a^{1/n} &= a^{p^f/n} = a^{(p^f-1)/n} \cdot a^{1/n} = \left(\frac{a}{p^f}\right)_n a^{1/n}, \\ \sigma_p^f a^{1/n} &= \left(\frac{a}{p^f}\right)_n a^{1/n}; \qquad a \in GF(p^f). \end{aligned} \tag{1.3}$$

Das Restsymbol $(a/p^f)_n$ ist also gerade der Faktor, den eine solche n-te Wurzel bei Anwendung von σ_p^f aufnimmt.

Nun sei $q \neq p$ eine weitere n nicht teilende rationale Primzahl und g ein zu n und q gehöriger Exponent

$$q^g \equiv 1(n), \quad q \neq p. \tag{1.1'}$$

Aus den Galoisfeldern $GF(p^f)$ bzw. $GF(q^g)$ wählen wir jeweils eine beliebige feste primitive n-te Einheitswurzel $\eta_{n,p}$ bzw. $\eta_{n,q}$ aus und identifizieren diese miteinander

$$\eta_{n,p} = \eta_{n,q} = \eta_n \in GF(p^f), GF(q^g). \tag{1.4}$$

Dann enthalten beide Galoisfelder dieselben n-ten Einheitswurzeln, nämlich die Potenzen von η_n.

Der Eulercharakter $\chi = \chi_{p^f,n}$ ist also in beiden Galoisfeldern erklärt, somit auch die mit ihm gebildeten "Kummer-Summen" (K-Summen)

$$K_{r,s} = {}_n^{p^f}K_{r,s} = \sum_{v \in GF(p^f)} \chi^r(v)\,\chi^s(v+1) \in GF(p^f), GF(q^g); \qquad r, s \in \mathbb{Z}. \tag{1.5}$$

Auf die Indices r, s kommt es offensichtlich nur modulo n an, sie seien stets so gemeint.

Gilt mindestens eine der Kongruenzen r, s, $r + s \equiv O(n)$, so sind die zugehörigen "trivialen K-Summen" direkt berechenbar. Man erhält[1]

$$\begin{aligned} K_{r,s} &= -1; && r + s \equiv O(n), r \not\equiv O(n), \\ &= -1; && r \equiv O(n), s \not\equiv O(n), \\ &= -\chi^r(-1); && r \not\equiv O(n), s \equiv O(n), \\ &= p^f - 2; && r \equiv s \equiv O(n). \end{aligned} \tag{1.6}$$

[1] Wenn nicht anders angegeben, gelten solche Formeln stets in $GF(p^f)$ und $GF(q^g)$. Das Indexpaar p^f, n schreiben wir nur, wenn es zum Verständnis notwendig ist.

Wir interessieren uns für die restlichen "nichttrivialen K-Summen" $K_{r,s}$; r, s, $r+s \not\equiv O(n)$. Auch diese sind als Elemente von $GF(p^f)$ leicht auszurechnen. Es gilt für[2] $f=1$—(A.1)—

$$ {}_n^p K_{r,s} = -\binom{sm}{(n-r)m} \in \mathbb{Z}_p,\ m=\frac{p-1}{n}; \qquad 0<r,s<n. \tag{1.7} $$

und damit

$$ {}_n^p K_{r,s} = 0 \in \mathbb{Z}_p \Leftrightarrow r+s<n; \qquad 0<r,s<n. \tag{1.7'} $$

Zwischen den K-Summen bestehen die einfachen Beziehungen—(A.4)—

$$ \begin{aligned} K_{r,s} &= \chi^{r+s}(-1)\,K_{s,r} = K_{-(r+s),s} = \chi^{r+s}(-1)\,K_{-(r+s),r} \\ &= \chi^{r}(-1)\,K_{s,-(r+s)} = \chi^{r}(-1)\,K_{r,-(r+s)} \end{aligned} \tag{1.8} $$

insbesondere gilt

$$ K_{1,s} = \chi(-1)\,K_{1,-(s+1)}. \tag{1.8'} $$

Mit einer beliebigen festen primitiven p-ten Einheitswurzel ξ aus dem p-ten Kreiskörper $GF(q^l)$ über $GF(q^g)$ bilden wir zu den Potenzen χ^r des Eulercharakters $\chi_{p^f,n}$ die "Gauß'schen Summen" (Stickelberger [8])

$$ {}_aG_r = \sum_{v \in GF(p^f)} \chi^r(v)\,\xi^{S(av)} \in GF(q^l); \qquad r \in \mathbb{Z},\ 0 \neq a \in GF(p^f), \tag{1.9} $$

wobei S die Spurbildung in den Primkörper $\mathbb{Z}_p$ bedeutet. Durch Summationstransformation— mit v durchläuft auch $a^{-1}v$ das $GF(p^f)$—erhält man

$$ {}_aG_r = \chi^{-r}(a)\,G_r; \qquad {}_1G_r = G_r. \tag{1.9'} $$

Ferner gilt für die "nichttrivialen Gauß'schen Summen" G_r; $r \not\equiv O(n)$ die "Betragsformel"[3]—(A.13)—

$$ G_r G_{-r} = \chi^r(-1)\cdot p^f; \qquad r \not\equiv O(n) \tag{1.10} $$

und für die zum "Hauptcharakter"[3] $\varepsilon=\chi^0$ gehörige "triviale Gauß'sche Summe"

$$ G_0 = -1. \tag{1.10'} $$

[2] Siehe auch Burde [2, §1, (4)] und für beliebiges f—was hier nicht benötigt wird— Burde [4, §3, Satz 15].

[3] Für die analog im Komplexen gebildeten Summen ist ${}_{-1}G^*_{-r} = \chi^{*r}(-1)\,G^*_{-r} = \bar{G}^*_r$ konj.-kompl. zu G^*_r und (1.10) geht über in $G^*_r \bar{G}^*_r = |G^*_r|^2 = p^f$. Für den Hauptcharakter $\varepsilon=\chi^0$ gelte $\varepsilon(0)=\chi^0(0)=0^0=0$.

Zwischen den nichttrivialen Gauß'schen—und K-Summen besteht der grundlegende Zusammenhang—(A.13)—

$$G_r \cdot G_s = \chi^r(-1)\, K_{r,s} \cdot G_{r+s}; \qquad r, s, r+s \not\equiv O(n), \tag{1.11}$$

oder aufgelöst nach der K-Summe (wegen (1.10) ist $G_{r+s} \neq 0$)

$$K_{r,s} = \chi^r(-1)\frac{G_r G_s}{G_{r+s}} \in GF(q^g); \qquad r, s, r+s \not\equiv O(n). \tag{1.12}$$

Über (1.12) erhält man aus (1.10) die "Betragsformel" für nichttriviale K-Summen

$$ {}_n^{p^f}K_{r,s} \cdot {}_n^{p^f}K_{-r,-s} = p^f; \qquad r, s, r+s \not\equiv O(n). \tag{1.13}$$

Mehrfache Anwendung von (1.11) liefert mit (1.6)

$$G^n = \chi(-1)\, p^f \prod_{s=1}^{n-2} K_{1,s} \in GF(q^g); \qquad G = G_1, \tag{1.14}$$

die n-te Potenz der Gauß'schen Summe $G = {}_1G_1$ liegt also bereits in $GF(q^g)$. Wendet man auf (1.14) den Eulercharakter $\psi = \chi_{q^g,n}$ an, so erhält man

$$\psi(G^n) = \psi(\chi(-1)) \cdot \psi(p^f) \cdot \psi\left(\prod_{s=1}^{n-2} K_{1,s}\right). \tag{1.15}$$

Die Reziprozität entspringt nun dem Verhalten der linken Seite in (1.15). Mit $a = G^n \in GF(q^g)$ und $\sigma_q^g \chi(v) = \chi(v)$; $\chi(v) \in GF(q^g)$, also nach (1.9) und (1.9′)

$$\sigma_q^g a^{1/n} = \sum_{v \in GF(p^f)} \chi(v)\, \zeta^{q^g S(v)} = {}_{q^g}G = \chi^{-1}(q^g) \cdot G,$$

folgt nach (1.3)

$$\psi(G^n) = \chi^{-1}(q^g). \tag{1.16}$$

Dies ist die eigentliche Reziprozitätsformel. Setzt man (1.16) in (1.15) ein, so erhält man das "Reziprozitätsgesetz für n-te Potenzreste in Galoisfeldern"

$$\left(\frac{q^g}{p^f}\right)_n \left(\frac{p^f}{q^g}\right)_n \left(\frac{(-1/p^f)_n}{q^g}\right)_n \prod_{s=1}^{n-2} \left(\frac{{}_n^{p^f}K_{1,s}}{q^g}\right)_n = 1. \tag{1.17}$$

Die Form dieses Gestzes kann man noch etwas verbessern, indem man die

Anzahl—und z.T. auch die Ordnungen—der beteiligten Restsymbole verringert. Mit (1.8′) und $\chi(-1)=1$; $n\equiv 1(2)$ wird (1.17) zu

$$\left(\frac{q^g}{p^f}\right)_n\left(\frac{p^f}{q^g}\right)_n\left(\frac{{}_n^{p^f}K_{1,(n-1)/2}}{q^g}\right)_n\prod_{s=1}^{(n-3)/2}\left(\frac{{}_n^{p^f}K_{1,s}}{q^g}\right)_n^2=1;\qquad n\equiv 1(2),\quad (1.18)$$

$$\left(\frac{q^g}{p^f}\right)_n\left(\frac{p^f}{q^g}\right)_n\left(\frac{(-1/p^f)_n}{q^g}\right)_n^{n/2}\prod_{s=1}^{(n-2)/2}\left(\frac{{}_n^{p^f}K_{1,s}}{q^g}\right)_{n/2}=1;\qquad n\equiv 0(2),\quad (1.18')$$

wobei das wegen

$$\left(\frac{(-1/p^f)_n}{q^g}\right)_n=(-1)^{(p^f-1)/n\cdot(q^g-1)/n}=\left(\frac{(-1/q^g)_n}{p^f}\right)_n \qquad (1.18'')$$

in p und q symmetrische Vorzeichensymbol in (1.18′) nur für $n\equiv 2(4)$ von 1 verschieden sein kann.

Speziell für Zweierpotenzen $n=2^r$; $r\geqslant 2$ läßt sich (1.18′) noch weiter "verbessern." Mit

$${}_{2^r}^{p^f}K_{2^{r-s},2^{r-s}}={}^{p^f}K_s=\sum_{v\in GF(p^f)}\left(\frac{v}{p^f}\right)_{2^s}\left(\frac{v+1}{p^f}\right)_{2^s};\qquad s\leqslant r \quad (1.19)$$

gilt nach (1.12)

$$\prod_{s=1}^{(n-2)/2}{}_{2^r}^{p^f}K_{1,s}=\pm\frac{G_1^{n/2}}{G_{n/2}}=\pm\prod_{j=0}^{r-2}{}_{2^r}^{p^f}K_{2^j,2^j}^{2^{(r-2)-j}}=\pm\prod_{s=2}^{r}{}^{p^f}K_s^{2^{s-2}}.$$

Setzt man dies in (1.18′) ein, so erhält man wegen

$$\left(\frac{-1}{q^g}\right)_{n/2}=\left(\frac{-1}{q^g}\right)_n^2=1$$

das "Reziprozitätsgesetz für Zweierpotenzen"

$$\left(\frac{p^f}{q^g}\right)_{2^r}\left(\frac{q^g}{p^f}\right)_{2^r}\prod_{s=2}^{r}\left(\frac{{}^{p^f}K_s}{q^g}\right)_{2^{r-s+1}}=1;\qquad r\geqslant 2. \qquad (1.20)$$

Es empfiehlt sich, die Exponenten f, g in diesen Reziprozitätsgesetzen stets minimal zu wählen, da die Aussage dann am schärfsten wird und, wie man leicht nachrechnet, die entsprechenden Aussagen bei größeren f, g enthält.

2. Komplexe Reziprozitätsgesetze

Die Exponenten f, g zu n und p bzw. q seien minimal gewählt. Im komplexen n-ten Kreiskörper

$$\mathbb{Q}_n=\mathbb{Q}(\xi_n);\qquad \xi_n=e^{2\pi i/n}.$$

zerfallen dann p und q bekanntlich in $t=\varphi(n)/f$ bzw. $l=\varphi(n)/g$ Primideale vom Grad f bzw. g

$$\begin{aligned} p &= \mathfrak{p}^{(1)} \cdots \mathfrak{p}^{(t)},\ N\mathfrak{p}^{(j)} = p^f; \qquad j=1,\ldots,t=\varphi(n)/f, \\ q &= \mathfrak{q}^{(1)} \cdots \mathfrak{q}^{(l)},\ N\mathfrak{q}^{(k)} = q^g; \qquad k=1,\ldots,l=\varphi(n)/g. \end{aligned} \tag{2.1}$$

Die Restklassenbereiche modulo $\mathfrak{p}^{(j)}$ bzw. $\mathfrak{q}^{(k)}$ sind also isomorph zu $GF(p^f)$ bzw. $GF(q^g)$ und mögen mit diesen identifiziert werden. Mit * sei der Übergang von η_n zu ξ_n bezeichnet

$$GF(p^f), GF(q^g) \ni \eta_n \overset{*}{\mapsto} \xi_n \in \mathbb{C}$$

und mit $'$ die Ringhomomorphismen von $\mathfrak{o}_n = \mathbb{Z}[\xi_n]$ in $GF(p^f)$ bzw. $GF(q^g)$, die auf $\mathbb{Z}$ die Restklassenabbildungen modulo p bzw. modulo q sind und η_n in ξ_n überführen. Genau für ein Primidealpaar $\mathfrak{p}^{(j)}$, $\mathfrak{q}^{(k)}$, etwa $\mathfrak{p}=\mathfrak{p}^{(1)}$ und $\mathfrak{q}=\mathfrak{q}^{(1)}$, sind dann $'$ gerade die Restklassenabbildungen modulo $\mathfrak{p}$ bzw. $\mathfrak{q}$.[4]

$$\begin{aligned} \alpha' &= \alpha + \mathfrak{p} \in \mathfrak{o}_n/\mathfrak{p} = GF(p^f) \\ \alpha' &= \alpha + \mathfrak{q} \in \mathfrak{o}_n/\mathfrak{q} = GF(q^g) \end{aligned} \qquad \alpha \in \mathfrak{o}_n = \mathbb{Z}[\xi_n]. \tag{2.2}$$

Für die über das Eulerkriterium erklärten m-ten Potenzrestsymbole modulo $\mathfrak{p}$ bzw. $\mathfrak{q}$

$$\begin{aligned} \left(\frac{\alpha}{\mathfrak{p}}\right)_m &= \xi_n^{\mu(\alpha)} \equiv \alpha^{(Np-1)/m}(\mathfrak{p}) \\ \left(\frac{\alpha}{\mathfrak{q}}\right)_m &= \xi_n^{\nu(\alpha)} \equiv \alpha^{(Nq-1)/m}(\mathfrak{q}) \end{aligned} \qquad \alpha \in \mathfrak{o}_n,\ m/n \tag{2.3}$$

gilt—$\chi = \chi_{p^f,n}$, $\psi = \chi_{q^g,n}$—

$$\begin{aligned} \left(\frac{\alpha}{\mathfrak{p}}\right)_m &= \left(\frac{\alpha'}{p^f}\right)_m^* = (\chi^*(\alpha'))^{n/m} \\ \left(\frac{\alpha}{\mathfrak{q}}\right)_m &= \left(\frac{\alpha'}{q^g}\right)_m^* = (\psi^*(\alpha'))^{n/m} \end{aligned} \qquad \alpha \in \mathfrak{o}_n,\ m/n \tag{2.4}$$

und $\chi_{\mathfrak{p}}$: $\chi_{\mathfrak{p}}(\alpha) = \chi^*(\alpha')$; $\alpha \in \mathfrak{o}_n$ ist der "komplexe Eulercharakter modulo $\mathfrak{p}$ der Ordnung n." Die K-Summen $K_{r,s}$ bzw. K_s gehen bei Anwendung von * über in die komplexen K-Summen modulo $\mathfrak{p}$

[4] Die Wahl von $\eta_{n,p}, \eta_{n,q}$ entspricht somit der Auswahl eines—beliebigen—Primidealpaares $\mathfrak{p}, \mathfrak{q}$ aus (2.1).

$$K_{r,s}^* = \sum_{r \in GF(p^f)}{}' \chi^{*r}(v)\chi^{*s}(v+1) = \sum_{v \bmod p}{}' \chi_p^r(v)\chi_p^s(v+1) \in \mathbb{Q}_n,$$
$$p^f K_s^* = \sum_{r \in GF(p^f)}{}' \left(\frac{v}{p^f}\right)_{2^s}^* \left(\frac{v+1}{p^f}\right)_{2^s}^* = \sum_{v \bmod p}{}' \left(\frac{v}{p}\right)_{2^s} \left(\frac{v+1}{p}\right)_{2^s} \in \mathbb{Q}_{2^s}. \tag{2.5}$$

Für die Summen ${}^{p^f}K_s^*$ gilt genauer—(A.12)—

$$\left(\frac{-4}{p^f}\right)_{2^s}^* {}^{p^f}K_s^* \in Z_s = \mathbb{Q}(\xi_{2^s} - \xi_{2^s}^{-1}); \qquad s \geqslant 2 \tag{2.5'}$$

und für $s = 2, 3$ sogar—(A.12″)—

$${}^{p^f}K_s^* \in Z_s = \mathbb{Q}(\xi_{2^s} - \xi_{2^s}^{-1}); \qquad s = 2, 3. \tag{2.5''}$$

Durch Anwendung von * werden die Reziprozitätsgesetze (1.18), (1.18′) und (1.20) übergeführt in die "komplexen Reziprozitätsgesetze"

$$\left(\frac{Nq}{p}\right)_n \left(\frac{Np}{q}\right)_n \left(\frac{{}^{Np}_{n}K^*_{1,(n-1)/2}}{q}\right)_n \prod_{s=1}^{(n-3)/2} \left(\frac{{}^{Np}_{n}K^*_{1,s}}{q}\right)_n^2 = 1; \qquad n \equiv 1(2), \tag{2.6}$$

$$\left(\frac{Nq}{p}\right)_n \left(\frac{Np}{q}\right)_n \left(\frac{(-1/p)_n}{q}\right)_n^{n/2} \prod_{s=1}^{(n-2)/2} \left(\frac{{}^{Np}_{n}K^*_{1,s}}{q}\right)_{n/2} = 1; \qquad n \equiv 0(2) \tag{2.6'}$$

mit

$$\left(\frac{(-1/p)_n}{q}\right)_n = (-1)^{(Np-1)/n \cdot (Nq-1)/n} = \left(\frac{(-1/q)_n}{p}\right)_n \tag{2.6''}$$

und

$$\left(\frac{Np}{q}\right)_{2^r} \left(\frac{Nq}{p}\right)_{2^r} \prod_{s=2}^{r} \left(\frac{{}^{Np}K_s^*}{q}\right)_{2^{r-s+1}} = 1; \qquad r \geqslant 2. \tag{2.7}$$

Vertauscht man in diesen Reziprozitätsgesetzen die Rollen von p und q, so erhält man—mit (2.6″)—aus Symmetriegründen die weiteren komplexen Reziprozitätsformeln

$$\left(\frac{{}^{Np}_{n}K^*_{1,(n-1)/2}}{q}\right)_n \prod_{s=1}^{(n-3)/2} \left(\frac{{}^{Np}_{n}K^*_{1,s}}{q}\right)_n^2 = \left(\frac{{}^{Nq}_{n}K^*_{1,(n-1)/2}}{p}\right)_n \prod_{s=1}^{(n-3)/2} \left(\frac{{}^{Nq}_{n}K^*_{1,s}}{p}\right)_n^2; \qquad n \equiv 1(2), \tag{2.8}$$

$$\prod_{s=1}^{(n-2)/2} \left(\frac{{}^{Np}_{n}K^*_{1,s}}{q}\right)_{n/2} = \prod_{s=1}^{(n-2)/2} \left(\frac{{}^{Nq}_{n}K^*_{1,s}}{p}\right)_{n/2}; \qquad n \equiv 0(2) \tag{2.8'}$$

und

$$\prod_{s=2}^{r}\left(\frac{{}^{Np}K_s^*}{\mathfrak{q}}\right)_{2^{r-s+1}}=\prod_{s=2}^{r}\left(\frac{{}^{Nq}K_s^*}{\mathfrak{p}}\right)_{2^{r-s+1}};\qquad r\geqslant 2. \tag{2.9}$$

Die Betragsformel (1.13) wird für die hier auftretenden komplexen K-Summen—${}_n^{Np}K^*_{-r,-s}={}_n^{Np}\bar{K}^*_{r,s}$ ist konj.-kompl. zu ${}_n^{Np}K^*_{r,s}$—zu

$$\begin{aligned}{}_n^{Np}K^*_{1,s}\cdot{}_n^{Np}\bar{K}^*_{1,s}&={}^{Np}K_s^*\cdot{}^{Np}\bar{K}_s^*=N\mathfrak{p},\\ {}_n^{Nq}K^*_{1,s}\cdot{}_n^{Nq}\bar{K}^*_{1,s}&={}^{Nq}K_s^*\cdot{}^{Nq}\bar{K}_s^*=N\mathfrak{q}.\end{aligned} \tag{2.10}$$

Betrachten wir als Beispiel (2.9) für $r=2$, d.h.

$$\left(\frac{{}^{Np}K_2^*}{\mathfrak{q}}\right)_2=\left(\frac{{}^{Nq}K_2^*}{\mathfrak{p}}\right)_2. \tag{2.11}$$

Hierin sind $\mathfrak{p},\mathfrak{q}$ Primideale von $\mathbb{Q}(\xi_4)=\mathbb{Q}(i)$, also Hauptideale $\mathfrak{p}=(\pi)$, $\mathfrak{q}=(\kappa)$ des Gauß'schen Zahlringes $\mathbb{Z}[i]$, wobei π,κ echtkomplexe oder rationale Primelemente von $\mathbb{Z}[i]$ sind. (Erstere seien mit ungeradem Realteil gewählt.)

$$\begin{aligned}\mathfrak{p}=(\pi);\quad \pi=a+ib\in\mathbb{Z}[i],\ a\equiv 1(2),\ b\neq 0,\ N\mathfrak{p}=\pi\cdot\bar{\pi}=p,\ f=1,\\ =p\in\mathbb{Z},\qquad 0<p\equiv 3(4),\quad N\mathfrak{p}=p^2,\qquad f=2,\end{aligned} \tag{2.12}$$

$$\begin{aligned}\mathfrak{q}=(\kappa),\quad \kappa=c+id\in\mathbb{Z}[i],\ c\equiv 1(2),\ d\neq 0,\ N\mathfrak{q}=\kappa\bar{\kappa}=q,\ g=1,\\ =q\in\mathbb{Z},\qquad 0<q\equiv 3(4),\quad N\mathfrak{q}=q^2,\qquad g=2.\end{aligned} \tag{2.12'}$$

Im Fall $f=1$ ist, wie aus (2.5) und (2.10)

$${}^pK_2^*\,{}^p\bar{K}_2^*=p,\qquad {}^pK_2^*\in\mathbb{Z}[i]$$

folgt, ${}^pK_2^*$ in $\mathbb{Z}[i]$ assoziiert zu π oder $\bar{\pi}$. Aus (1.7') ergibt sich mit $\mathbb{Z}_p=\mathbb{Z}[i]/(\pi)$ die Kongruenz

$${}^pK_2^*={}_4^pK^*_{1,1}\equiv 0(\pi),$$

wegen $\bar{\pi}\not\equiv 0(\pi)$ ist daher ${}^pK_2^*$ zu π assoziiert, genauer gilt—(A.14*)—

$${}^pK_2^*=\pm\pi;\qquad f=1. \tag{2.13'}$$

Für $f=2$ erhält man mit der Summationstransformation $v \mapsto \sigma_p v = v^p$; $v \in GF(p^2)$ wegen $v^p + 1 = (v+1)^p$ und $p \equiv 3(4)$

$$ {}^{p^2}K_2^* = \sum_{v \in GF(p^2)} \left(\frac{v}{p^2}\right)_4^{*p} \left(\frac{v+1}{p^2}\right)_4^{*p} = {}^{p^2}\bar{K}_2^*, $$

d.h. ${}^{p^2}K_2^* \in \mathbb{Z}$ und nach (2.10) ${}^{p^2}K_2^{*2} = p^2$, somit

$$ {}^{p^2}K_2^* = \pm p = \pm\pi; \qquad f=2. $$

Entsprechendes gilt für ${}^{Nq}K_2^*$, man hat also

$$ {}^{Np}K_2^* = \pm\pi, \ {}^{Nq}K_2^* = \pm\kappa; \qquad \mathfrak{p} = (\pi), \ \mathfrak{q} = (\kappa) \tag{2.13} $$

und mit[5]

$$ \left(\frac{-1}{\mathfrak{p}}\right)_2 = \left(\frac{-1}{p}\right) = 1; \qquad p = N\pi \equiv 1(4), f = 1, $$

$$ = \left(\frac{-1}{(p)}\right)_2 = \left(\frac{-1}{p}\right)^{p+1} = 1; \qquad p \equiv 3(4), \qquad f = 2 $$

erweist sich (2.11) als das komplexe quadratische Reziprozitätsgesetz im Gauß'schen Zahlkörper $\mathbb{Q}(i)$

$$ \left(\frac{\pi}{\kappa}\right)_2 = \left(\frac{\kappa}{\pi}\right)_2, $$

für verschiedene—echt-komplexe oder rationale— Priemelemente von $\mathbb{Z}[i]$ (erstere mit ungeradem Realteil).

Für das Weitere beschränken wir uns auf den Fall $f = g = 1$, also p, $q \equiv 1(n)$. Sei $\mathfrak{p}$ wieder das zu $\eta_n = \eta_{n,p}$ gehörige Primideal aus $\mathbb{Q}_n$ (vom Grad 1) und Z ein Zwischenkörper

$$ \mathbb{Q} \subset Z \subset \mathbb{Q}_n. $$

Die Restriktion der Restklassenabbildung $'$ modulo $\mathfrak{p}$ auf Z bzw. auf den Ganzheitsring $\mathfrak{o}_Z = \mathfrak{o}_n \cap Z$ ist genau für das unter $\mathfrak{p}$ liegende Primideal $\mathfrak{p}_Z$ aus $\mathfrak{o}_Z$ Restklassenabbildung. Z enthalte die m-ten Einheitswurzeln für m/n, sodaß die—über das Eulerkriterium erklärten—m-ten Restsymbole modulo $\mathfrak{p}_Z$ bildbar seien. Dann gilt für $f=1$ nach (2.4)[6]

$$ \left(\frac{\alpha}{\mathfrak{p}_Z}\right)_m \equiv \left(\frac{\alpha'}{p}\right)_m^*; \qquad \alpha \in \mathfrak{o}_Z, \ \mathbb{Q}_m \subset Z, $$

[5] Restsymbole ohne Index sind Legendre- bzw. Jacobi-Symbole.

[6] Für $f > 1$ gilt dies nicht allgemein, da dann der Fall $1 \leqslant \text{Grad } \mathfrak{p}_Z < \text{Grad } \mathfrak{p} = f > 1$ eintreten kann.

also

$$\left(\frac{\alpha}{\mathfrak{p}}\right)_m = \left(\frac{\alpha}{\mathfrak{p}_Z}\right)_m; \qquad \alpha \in \mathfrak{o}_Z,\ \mathbb{Q}_m \subset Z \subset \mathbb{Q}_n. \tag{2.14}$$

Betrachten wir nun (2.9) für $r = 3$, also $n = 2^3 = 8$, und $f = g = 1$, also p, $q \equiv 1(8)$:

$$\left(\frac{{}^pK_2^*}{\mathfrak{q}}\right)_4 \left(\frac{{}^pK_3^*}{\mathfrak{q}}\right)_2 = \left(\frac{{}^qK_2^*}{\mathfrak{p}}\right)_4 \left(\frac{{}^qK_3^*}{\mathfrak{p}}\right)_2; \qquad N\mathfrak{p} = p \equiv 1(8), N\mathfrak{q} = q \equiv 1(8). \tag{2.15}$$

Oben hatten wir es bereits mit den Quadraten der hierin auftretenden biquadratischen Symbole, d.h. mit den entsprechenden quadratischen Symbolen zu tun. Nach (2.13) gilt mit den dortigen—echt-kompl.—Primelementen $\pi, \kappa \in \mathbb{Z}[i]$ offenbar $(\pi) = \mathfrak{p}_{\mathbb{Q}(i)}$ und $(\kappa) = \mathfrak{q}_{\mathbb{Q}(i)}$, also wegen

$$\left(\frac{-1}{\mathfrak{p}}\right)_4 = \left(\frac{-1}{p}\right)_4 = 1; \qquad p \equiv 1(8)$$

nach (2.14)

$$\left(\frac{{}^pK_2^*}{\mathfrak{q}}\right)_4 = \left(\frac{\pi}{\kappa}\right)_4, \qquad \left(\frac{{}^qK_2^*}{\mathfrak{p}}\right)_4 = \left(\frac{\kappa}{\pi}\right)_4. \tag{2.16}$$

Wenden wir uns den quadratischen Symbolen in (2.15) zu. Nach (2.5″) und (2.10) gilt

$${}^pK_3^*{}^p\bar{K}_3^* = p,\ {}^qK_3^*{}^q\bar{K}_3^* = q; \qquad {}^pK_3^*, {}^qK_3^* \in Z_3 = \mathbb{Q}(\xi_8 - \xi_8^{-1}) = \mathbb{Q}(\sqrt{-2}).$$

Da die Primzahlen p, $q \equiv 1(8)$ in $\mathbb{Q}(\sqrt{-2})$ im wesentlichen, d.h. bis auf Reihenfolge und Vorzeichen der Faktoren, eindeutig in das Produkt zweier Primelemente zerfallen

$$p = \pi' \cdot \bar{\pi}',\ q = \kappa' \cdot \bar{\kappa}'; \qquad \pi', \kappa' \in \mathbb{Q}(\sqrt{-2}),$$

hat man nach Obigem etwa

$${}^pK_3^* = \pm\pi', \qquad {}^qK_3^* = \pm\kappa',$$

und dann wegen

$${}^pK_3^* = {}_8^pK_{1,1}^* = \pm\pi' \equiv O(\mathfrak{p}_{Z_3}),$$

wie aus (1.7′) mit $\mathbb{Z}_p = \mathfrak{o}_8/\mathfrak{p} = \mathfrak{o}_{Z_3}/\mathfrak{p}_{Z_3}$ folgt, aber $\pi' \not\equiv O(\bar{\pi}')$

$$\mathfrak{p}_{Z_3} = (\pi'), \qquad \mathfrak{q}_{Z_3} = (\kappa').$$

Mit $(-1/\mathfrak{p})_2 = (-1/p) = 1$ folgt daraus nach (2.14)

$$\left(\frac{{}^pK_3^*}{\mathfrak{q}}\right)_2 = \left(\frac{\pi'}{\kappa'}\right)_2, \qquad \left(\frac{{}^qK_3^*}{\mathfrak{p}}\right)_2 = \left(\frac{\kappa'}{\pi'}\right)_2$$

womit (2.15) die Form

$$\left(\frac{\pi}{\kappa}\right)_4 \left(\frac{\pi'}{\kappa'}\right)_2 = \left(\frac{\kappa}{\pi}\right)_4 \left(\frac{\kappa'}{\pi'}\right)_2 \tag{2.15′}$$

annimmt.

Nun gilt in $\mathbb{Q}(\sqrt{-2})$ die Umkehrformel[7]—(A.15)—

$$\left(\frac{\pi'}{\kappa'}\right)_2 = \left(\frac{\kappa'}{\pi'}\right)_2; \qquad p = \pi' \cdot \bar{\pi}' \equiv 1(8), q = \kappa' \cdot \bar{\kappa}' \equiv 1(8), \pi', \kappa' \in \mathbb{Q}(\sqrt{-2}). \tag{2.17}$$

Aus (2.15′) und (2.17) ergibt sich has Eisenstein'ssche biquadratische Reziprozitätsgesetz in $\mathbb{Q}(i)$ (Eisenstein [5])

$$\left(\frac{\pi}{\kappa}\right)_4 = \left(\frac{\kappa}{\pi}\right)_4; \qquad N\pi = p \equiv 1(8), N\kappa = q \equiv 1(8) \tag{2.18}$$

für den Fall zweier echt-komp. Primelemente $\pi, \kappa \in \mathbb{Z}[i]$—mit ungeraden Realteilen—deren Normen beide $\equiv 1(8)$ sind.

3. Rationale Reziprozitätsgesetze

Wir gehen wieder von den §1 hergeleiteten Reziprozitätsgesetzen aus. Um von diesen zu "rationalen Reziprozitätsgesetzen" zu kommen, beschränken wir und auf die "rationalen Restklassenbereiche" $\mathbb{Z}_p, \mathbb{Z}_q$, d.h. auf den Fall $f = g = 1$, und schreiben die auftretenden K-Summen "rational"—siehe (3.7) und (3.10). Betrachten wir das Reziprozitätsgesetz für Zweierpotenzen (1.20), das bei den rationalen Reziprozitätsgesetzen eine besondere Rolle spielt. Für $f = g = 1$ lautet es

$$\left(\frac{p}{q}\right)_{2^r} \left(\frac{q}{p}\right)_{2^r} \prod_{s=2}^{r} \left(\frac{{}^pK_s}{q}\right)_{2^{r-s+1}} = 1; \qquad p, q \equiv 1(2^r), r \geqslant 2. \tag{3.1}$$

[7] Diese folgt auch aus dem allgemeinen quadratischen Reziprozitätsgesetz in algebraischen Zahlkörpern von Hecke [6, §59].

Mit

$$ {}^{p}\bar{K}_s = \sum_{\nu \in \mathbb{Z}_p} \left(\frac{\nu}{p}\right)_{2^s}^{-1} \left(\frac{\nu+1}{p}\right)_{2^s}^{-1}; \qquad {}^{p}K_s = \sum_{\nu \in \mathbb{Z}_p} \left(\frac{\nu}{p}\right)_{2^s} \left(\frac{\nu+1}{p}\right)_{2^s} \tag{3.2} $$

erhält die Betragsformel (1.13) die Form

$$ {}^{p}K_s \cdot {}^{p}\bar{K}_s = p, \qquad {}^{q}K_s \cdot {}^{q}\bar{K}_s = q, \tag{3.3} $$

weiter gilt nach (1.7′)

$$ {}^{p}K_s = 0 \in \mathbb{Z}_p, \ {}^{q}K_s = 0 \in \mathbb{Z}_q; \qquad s \geqslant 2. \tag{3.4} $$

Wir versuchen nun, die K-Summen ${}^{p}K_s$; $s = 2, 3, \ldots$ rational zu schreiben, was sich für wachsendes s als immer schwieriger herausstellen wird.

$s = 2$. Faßt man in der Summendarstellung (3.2) die Summanden ± 1 und[8] $\pm\eta_4$ zusammen, so erhält man mit $\eta_4 = i$—(A.14)—

$$ \begin{aligned} &{}^{p}K_2 = a + ib, \ {}^{p}\bar{K}_2 = a - ib \in \mathbb{Z}_p, \mathbb{Z}_q \\ &{}^{q}K_2 = c + id, \ {}^{q}\bar{K}_2 = c - id \in \mathbb{Z}_p, \mathbb{Z}_q \end{aligned} \qquad a, c \equiv 1(2), \tag{3.5} $$

nach (3.3) somit

$$ \begin{aligned} p &= (a + ib)(a - ib) = a^2 + b^2 \in \mathbb{Z}_p, \mathbb{Z}_q, \\ q &= (c + id)(c - id) = c^2 + d^2 \in \mathbb{Z}_p, \mathbb{Z}_q. \end{aligned} $$

Bei gegebenem p, also auch gegebenen $a^2, b^2 \in \mathbb{Z}$, kann man nun—nach dem Primzahlsatz von Dirichlet—$q \equiv 1(2^r)$ größer als $a^2 + b^2$ wählen. Mit einem solchen q folgt aus Obigem die exakte Gleichung $p = a^2 + b^2$ in $\mathbb{Z}$. Entsprechendes gilt für q

$$ p = a^2 + b^2, \ q = c^2 + d^2; \qquad a, c \equiv 1(2). \tag{3.6} $$

Diese Quadratsummendarstellungen sind bekanntlich bis auf das Vorzeichen von $a, b, c, d \in \mathbb{Z}$ eindeutig.

Aus (3.5) und (3.4) folgt $c + id = 0 \in \mathbb{Z}_q$, also $i = -c/d \in \mathbb{Z}_q$ und damit

$$ {}^{p}K_2 = a - \frac{c}{d} b = \frac{1}{d}(ad - bc) \in \mathbb{Z}_q $$

$$ {}^{p}K_2 = \frac{1}{d}(ad - bc) \in \mathbb{Z}_q; \qquad p = a^2 + b^2, \ q = c^2 + d^2, \ a, c \equiv 1(2), \tag{3.7} $$

[8] $\eta_{2^s} = \eta_{2^r}^{2^{r-s}}$; $n = 2^r$, $s \leqslant r$.

wobei die noch offenen Vorzeichen von a, b, c, d von der Wahl von $\eta_4 = i$, genauer von der Zuordnung von $\eta_{4,p}$ zu $\eta_{4,q}$ abhängen. Dies ist die oben gemeinte "rationale Schreibweise" von ${}^pK_2$.

$s = 3$. Faßt man in der Summendarstellung (3.2) die Einheitswurzelsummanden mit ihren jeweils additiv Inversen zusammen, so erhält man mit $\eta_8^4 = -1$

$$ {}^pK_3 = x + y\eta_8 + z\eta_8^2 + w\eta_8^3; \qquad x, y, z, w \in \mathbb{Z}. $$

Da ${}^pK_3$ invariant gegenüber der Substitution τ_3: $\eta_8 \mapsto \eta_8^3$ ist—(A.10′)—gilt auch

$$ {}^pK_3 = \tau_3 {}^pK_3 = x + y\eta_8^3 - z\eta_8^2 + w\eta_8, \tag{3.8′} $$

also

$$ 2 \cdot {}^pK_3 = 2x + (y + w)(\eta_8 + \eta_8^3), \tag{3.8} $$

entsprechend

$$ 2 \cdot {}^p\bar{K}_3 = 2x - (y + w)(\eta_8 + \eta_8^3). $$

Mit $(\eta_8 + \eta_8^3)^2 = -2$ liefert nun (3.3)

$$ 4p = 4x^2 + 2(y + w)^2 \in \mathbb{Z}_q, $$

und diese Beziehung gilt, wie man wieder erkennt wenn man q hinreichend groß wählt, sogar in $\mathbb{Z}$. Mit $A = x$ und $B = \frac{1}{2}(y + w) \in \mathbb{Z}$—$(y + w)$ muß gerade sein—hat man also für p die Quadratsummendarstellung $p = A^2 + 2B^2$; A, $B \in \mathbb{Z}$ in $\mathbb{Z}$ und nach (3.8) ${}^pK_3 = A + B(\eta_8 + \eta_8^3)$. Entsprechendes gilt für ${}^qK_3$

$$ \begin{aligned} &{}^pK_3 = A + B(\eta_8 + \eta_8^3) \in \mathbb{Z}_p, \mathbb{Z}_q, \; p = A^2 + 2B^2 \\ &{}^qK_3 = C + D(\eta_8 + \eta_8^3) \in \mathbb{Z}_p, \mathbb{Z}_q, \; q = C^2 + 2D^2 \end{aligned} \qquad A, B, C, D \in \mathbb{Z} \tag{3.9} $$

und die hierin auftretenden Quadratsummendarstellungen von $p, q \equiv 1(8)$ sind bekanntlich bis auf das Vorzeichen von A, B, C, D eindeutig. An Hand von (3.9) ist es nun nicht mehr schwer, auch ${}^pK_3$ rational zu schreiben. Mit (3.4) erhält man aus (3.9) zunächst $(\eta_8 + \eta_8^3) = -C/D \in \mathbb{Z}_q$ und dann

$$ {}^pK_3 = A - \frac{C}{D}B = \frac{1}{D}(AD - BC) \in \mathbb{Z}_q, $$

d.h. eine zu (3.7) ganz analoge "rationale Schreibweise"

$$ {}^pK_3 = \frac{1}{D}(AD - BC) \in \mathbb{Z}_q; \quad p = A^2 + 2B^2, q = C^2 + 2D^2, A, B, C, D \in \mathbb{Z}, \tag{3.10} $$

in der die noch offenen Vorzeichen von A, B, C, D von der Wahl von $(\eta_8 + \eta_8^3)$ abhängen.

An Hand von (3.7) und (3.10) kann man in den Reziprozitätsgesetzen (3.1) die ersten beiden Restsymbole des Produktes rational schreiben. Für $r = 2, 3$ erhält man damit die rationalen Reziprozitätsgesetze für 4-te und 8-te Reste

$$\left(\frac{p}{q}\right)_4 \left(\frac{q}{p}\right)_4 \left(\frac{\frac{1}{2}(ad-bc)}{q}\right) = 1; \qquad p, q \equiv 1(4),^{9} \tag{3.11}$$

$$\left(\frac{p}{q}\right)_8 \left(\frac{q}{p}\right)_8 \left(\frac{ab-bc}{q}\right)_4 \left(\frac{AD-BC}{q}\right) = 1; \qquad p, q \equiv 1(8),^{10} \tag{3.12}$$

wobei $(d/q)_4 = 1$; $q \equiv 1(8)$—siehe etwa v. Lienen [7] (S. 91 in der Habilitationsschrift)—und—(A.17), (A.16)—

$$\left(\frac{d}{q}\right) = \left(\frac{2}{q}\right); \qquad q \equiv 1(4), \tag{3.11'}$$

$$\left(\frac{D}{q}\right) = 1; \qquad q \equiv 1(8) \tag{3.12'}$$

benutzt wurde. Für $r = 4$ ergibt sich[11]

$$\left(\frac{p}{q}\right)_{16} \left(\frac{q}{p}\right)_{16} \left(\frac{d(ad-bc)}{q}\right)_8 \left(\frac{D(AD-BC)}{q}\right)_4 \left(\frac{{}^pK_4}{q}\right) = 1; \qquad p, q \equiv 1(16) \tag{3.13}$$

und zu einer vollständigen Rationalisierung ist nur noch ${}^pK_4$ rational zu schreiben.

Die Rationalisierung von ${}^pK_s$ hängt, wie die durchgeführten Beispiele $s = 2, 3$ deutlich machen, eng mit der komplexen Zerlegung von p in $Z_s = \mathbb{Q}(\xi_{2^s} - \xi_{2^s}^{-1})$

$$p = {}^pK_s^* \, {}^p\bar{K}_s^*; \qquad \left(\frac{-4}{p}\right)_{2^s}^* {}^pK_s^* \overset{(2.5')}{\in} Z_s = \mathbb{Q}(\xi_{2^s} - \xi_{2^s}^{-1}) \tag{3.14}$$

zusammen (und läßt sich auch—unter Benutzung der Ergebnisse von §2—über diese Zerlegungen gewinnen).

Daß die Rationalisierung von ${}^pK_2$ und ${}^pK_3$ verhältnismäßig leicht gelingt, liegt nun daran, daß die Körper $Z_2 = \mathbb{Q}(i)$ und $Z_3 = \mathbb{Q}(\sqrt{-2})$ nur

[9] Burde, [1, 3]; Williams [10].
[10] Williams [9].
[11] Williams [11].

quadratisch über $\mathbb{Q}$ sind. Da $Z_4 = \mathbb{Q}(\xi_{16} - \xi_{16}^{-1})$ jedoch den Grad 4 über $\mathbb{Q}$ besitzt, wird die zugehörige Zerlegung (3.14) und dementsprechend auch die Rationalisierung von ${}^pK_4$ komplizierter. (Siehe hierzu Williams [11].)

Die bislang formulierten rationalen Reziprozitätsgesetze haben noch einen Schönheitsfehler. Die in ihnen auftretenden Restsymbole und K-Summen sind z.T. abhängig von der Wahl der Einheitswurzeln $\eta_{n,p}, \eta_{n,q}$, genauer von ihrer Zuordnung zueinander durch die Identifikation $\eta_{n,p} = \eta_{n,q} = \eta_n$. Fassen wir die Reziprozitätsgesetze des §1 etwa als Beziehungen in $GF(q^g)$ auf, so bleiben bei der Substitution

$$\rho_j : \eta_{n,q} \mapsto \eta_{n,q}^j,\ \eta_{n,p} \mapsto \eta_{n,p}; \qquad (j,n) = 1, \tag{3.15}$$

welche diese Zuordnung ändert, nur die Restsymbole mit dem "Nenner" q^g unverändert, nicht aber die Restsymbole mit dem Nenner p^f sowie die K-Summen ${}_n^{p^f}K_{r,s}$, ${}^{p^f}K_s$. Es gilt vielmehr in $GF(q^g)$

$$\rho_f\left(\frac{x}{p^f}\right)_n = \left(\frac{x}{p^f}\right)_n^j,\ \rho_j\left(\frac{y}{q^g}\right)_n = \left(\frac{y}{q^g}\right)_n,\ \rho_j\, {}_n^{p^f}K_{r,s} = {}_n^{p^f}K_{rj,sj} \qquad \begin{matrix} x \in GF(p^f) \\ y \in GF(q^g) \end{matrix} \tag{3.16}$$

und Entsprechendes nach (1.19) für ${}^{p^f}K_s \in GF(q^g)$.

Invariant gegenüber der Zuordnung der Einheitswurzel η zueinander ist das Symbol $(q^g/p^f)_n \in GF(q^g)$ somit genau nur dann, wenn es gleich ± 1 ist. Aus Symmetriegründen wird man diese Forderung auch an das reziproke Symbol stellen. Nichttriviale "streng rationale Reziprozitätsgesetze," in denen die Symbole unabhängig von der Zuordnung der Einheitswurzeln η zueinander sind, erhält man also nur unter der—symmetrischen—Voraussetzung $(f = g = 1)$

$$\left(\frac{q}{p}\right)_{n/2} = \left(\frac{p}{q}\right)_{n/2} = 1, \qquad n \equiv 0(2). \tag{3.17}$$

Dies zeigt, daß solche streng rationalen Reziprozitätsgesetze überhaupt nur für Zweierpotenzen sinnvoll sind.

Unter den zugehörigen Voraussetzungen (3.17) gehen (3.11) in das früher bereits einmal von mir formulierte (Burde [1]), (3.12) und—nach Rationalisierung von ${}^pK_4$—(3.13) in die kürzlich von Williams [9, 11] hergeleiteten streng rationalen Reziprozitätsgesetze für 4-te, 8-te und 16-te Potenzreste über, in denen es dann auf die—von der Wahl der Einheitswurzeln η abhängigen—Vorzeichen der Zerlegungskoeffizienten a, b, c, d bzw. A, B, C, D nicht mehr ankommt. Aus den Reziprozitätsgesetzen des §1 kann man natürlich weitere—für $n \neq 2^r$ nicht streng—rationale Reziprozitätsgesetze herleiten, wie etwa das von v. Lienen [7] aufgestellte rationale kubische Reziprozitätsgesetz (siehe hierzu Burde [3]).

ANHANG

Beweis von (1.7)

Für die K-Summe ${}_n^p K_{r,s}$ gilt nach (1.5) und (1.2) für $f=1$, also $p \equiv 1(n)$

$$ {}_n^p K_{r,s} = \sum_{v \in \mathbb{Z}_p} v^{rm}(v+1)^{sm} = \sum_{j=0}^{p-1} \binom{sm}{j} \sum_{v \in \mathbb{Z}_p^*} v^{rm+j} \in \mathbb{Z}_p; $$

$$ m = \frac{p-1}{n}, \quad 0 < r, s < n. $$

Wegen

$$ 0 < rm + j < 2(p-1); \qquad r = 1,\ldots, n-1, j = 0,\ldots, p-1 $$

erhält man für die innere Summe von $(p-1)$-ten Einheitswurzeln

$$ \sum_{v \in \mathbb{Z}_p^*} v^{rm+j} = p-1 = -1 \in \mathbb{Z}_p; \qquad j = (p-1) - rm = (n-r)m, $$
$$ = 0 \in \mathbb{Z}_p; \qquad \text{sonst.} $$

Das liefert

$$ {}_n^p K_{r,s} = -\binom{sm}{(n-r)m} \in \mathbb{Z}_p; \qquad m = \frac{p-1}{n}, \ 0 < r, s < n. \tag{A.1} $$

Beweis von (1.8), (2.5′), (2.5″), (3.8′)

Für die K-Summe

$$ K_{r,s} = \sum_{v \in GF(p^f)} \chi^r(v)\chi^s(v+1) = \sum_{v \in GF^*(p^f)} \chi^r(v)\chi^s(v+1) $$

erhält man über die Summationstransformation: $v \mapsto 1/v$

$$ K_{r,s} = \sum_{v \in GF^*(p^f)} \chi^r\left(\frac{1}{v}\right)\chi^s\left(\frac{1}{v}+1\right) = \sum_{v \in GF^*(p^f)} \chi^r\left(\frac{1}{v}\right)\chi^s\left(\frac{1+v}{v}\right) $$
$$ = \sum_{v \in GF^*(p^f)} \chi^{-(r+s)}(v)\chi^s(v+1) = K_{-(r+s),s}, $$
$$ K_{r,s} = K_{-(r+s),s}. \tag{A.2} $$

Anwendung der Summationstransformation: $v \mapsto -(v+1)$ liefert

$$ K_{r,s} = \sum_{v \in GF(p^f)} \chi^r(-(v+1))\chi^s(-(v+1)+1) $$
$$ = \chi^{r+s}(-1) \sum_{v \in GF(p^f)} \chi^s(v)\chi^r(v+1) = \chi^{r+s}(-1) K_{s,r}, $$
$$ K_{r,s} = \chi^{r+s}(-1) K_{s,r}. \tag{A.3} $$

Aus (A.2) und (A.3) ergibt sich

$$\begin{aligned} K_{r,s} &= \chi^{r+s}(-1)\, K_{s,r} = K_{-(r+s),s} = \chi^{r+s}(-1)\, K_{-(r+s),r} \\ &= \chi^{r}(-1)\, K_{s,-(r+s)} = \chi^{r}(-1)\, K_{r,-(r+s)}. \end{aligned} \tag{A.4}$$

Außerdem gilt die etwas tiefer liegende Beziehung

$$K_{-1,2} = \chi(-4)\, K_{n/2+1,n/2}; \qquad n \equiv 0(2). \tag{A.5}$$

Bew.:

$$K_{-1,2} = \sum_{v \in GF^*(p^f)} \chi^{-1}(v)\chi^2(v+1) = \sum_{v \in GF^*(p^f)} \chi(v+2+v^{-1}).$$

Wir berechnen, wie oft das Argument $v+2+v^{-1}$ den—wegen $p \neq 2$ beliebigen—Wert -2μ; $\mu \in GF(p^f)$ annimmt. $v+2+v^{-1} = -2\mu$ führt auf die quadratische Gleichung

$$v^2 + 2v(1+\mu) + 1 = 0$$

mit den Lösungen

$$v_{1,2} = -(1+\mu) \pm \sqrt{\mu(\mu+2)} \in GF^*(p^f).$$

Daraus folgt, daß der Wert -2μ genau

$$(1 + \chi^{n/2}(\mu(\mu+2)))$$

mal angenommen wird. Somit gilt

$$\begin{aligned} K_{-1,2} &= \sum_{\mu \in GF(p^f)} (1 + \chi^{n/2}(\mu(\mu+2)))\chi(-2\mu) \\ &= \chi(-2) \sum_{\mu \in GF(p^f)} \chi^{n/2+1}(\mu)\chi^{n/2}(\mu+2) \qquad \sum_{\mu \in GF(p^f)} \chi(-2\mu) = 0. \\ &= \chi(-2) \sum_{\mu \in GF(p^f)} \chi^{n/2+1}(2\mu)\chi^{n/2}(2\mu+2) \\ &= \chi(-4) \sum_{\mu \in GF(p^f)} \chi^{n/2+1}(\mu)\chi^{n/2}(\mu+1) = \chi(-4)\, K_{n/2+1,n/2}. \end{aligned}$$

Aus (A.4) und der Betragsformel (1.13) folgt

$$K_{-1,2} = \chi(-1)\, p^f \cdot K_{1,1}^{-1}, \qquad K_{n/2+1,n/2} = \chi(-1)\, p^f \cdot K_{1,n/2-1}^{-1},$$

nach (A.5) somit

$$K_{1,n/2-1} = \chi(-4)\, K_{1,1}. \tag{A.6}$$

Mit

$$\tau_j K_{r,s} = K_{rj,sj};\ \tau_j\colon \eta_n \mapsto \eta_n^j, \qquad (j,n)=1 \tag{A.7}$$

erhält man wegen

$$\chi(-1)=1,\ \left(\frac{n}{2}-1\right)^2 = \frac{n^2}{4} - n + 1 \equiv 1(n); \qquad n \equiv 0(4)$$

nach (A.4)

$$\begin{aligned} \tau_{n/2-1} K_{1,n/2-1} &= K_{n/2-1,1} = K_{1,n/2-1}, \\ \tau_{n/2-1} K_{1,n/2-1} &= K_{1,n/2-1}; \qquad n \equiv 0(4). \end{aligned} \tag{A.8}$$

Aus (A.6) und (A.8) ergibt sich

$$\tau_{n/2-1}(\chi(-4)\, K_{1,1}) = \chi(-4)\, K_{1,1}; \qquad n \equiv 0(4). \tag{A.9}$$

Nun gilt mit $\chi^{n/2}(4) = \chi^n(2) = 1$ und $\chi(-) = 1$; $n \equiv 0(4)$

$$\tau_{n/2-1}\chi(-4) = \chi^{n/2-1}(-4) = \chi^{-1}(-4),$$

also

$$\tau_{n/2-1}\chi(-4) = \chi(-4) \Leftrightarrow \chi^4(2) = 1, \tag{A.9'}$$

und damit

$$\tau_{n/2-1} K_{1,1} = K_{1,1};\ \chi^4(2) = 1, \qquad n \equiv 0(4). \tag{A.10}$$

Für $n = 8$ und $p \equiv 1(8)$, also $f = 1$, erhält man aus (A.10) mit ${}_8^p K_{1,1} = {}^p K_3$ und $\chi^4(2) = (2/p) = 1$; $p \equiv 1(8)$

$$\tau_3\, {}^p K_3 = {}^p K_3. \tag{A.10'}$$

Gehen wir durch Anwendung von *: $\eta_n \mapsto \xi_n$ zum Komplexen über, so wird aus τ_j der Automorphismus

$$\tau_j^*\colon \xi_n \mapsto \xi_n^j; \qquad (j,n)=1$$

von $\mathbb{Q}_n$ und (A.9), (A.10) gehen über in

$$\tau^*_{n/2-1}(\chi^*(-4)\, K^*_{1,1}) = \chi^*(-4)\, K^*_{1,1} \in \mathbb{Q}_n; \qquad n \equiv 0(4), \tag{A.9*}$$

$$\tau^*_{n/2-1} K^*_{1,1} = K^*_{1,1} \in \mathbb{Q}_n;\ \chi^{*4}(2) = 1, \qquad n \equiv 0(4). \tag{A.10*}$$

Das bedeutet aber, da $\mathbb{Q}(\xi_n - \xi_n^{-1}) \subset \mathbb{Q}_n$ der Fixkörper der von $\tau^*_{n/2-1}$ erzeugten Untergruppe der Galoisgruppe von $\mathbb{Q}_n/\mathbb{Q}$ ist,

$$\chi^*(-4)\, K^*_{1,1} \in \mathbb{Q}(\xi_n - \xi_n^{-1}); \qquad n \equiv 0(4), \tag{A.11}$$

$$K^*_{1,1} \in \mathbb{Q}(\xi_n - \xi_n^{-1}); \qquad \chi^{*4}(2) = 1,\ n \equiv 0(4). \tag{A.11'}$$

Insbesondere hat man

$$\left(\frac{-4}{p^f}\right)^*_{2^s} {}^{p^f}K^*_s \in Z_s = \mathbb{Q}(\xi_{2^s} - \xi_{2^s}^{-1}); \qquad s \geqslant 2, \tag{A.12}$$

$${}^{p^f}K^*_s \in Z_s = \mathbb{Q}(\xi_{2^s} - \xi_{2^s}^{-1}); \qquad \left(\frac{2}{p^f}\right)^*_{2^{s-2}} = 1,\ s \geqslant 2. \tag{A.12'}$$

Für $s = 2, 3$ gilt offenbar $(2/p^f)^*_{2^{s-2}} = 1$, da für $s = 3$ entweder $f > 1$ oder $p \equiv 1(8)$ ist. Das liefert

$${}^{p^f}K^*_s \in Z_s = \mathbb{Q}(\xi_{2^s} - \xi_{2^s}^{-1}); \qquad s = 2, 3. \tag{A.12''}$$

Bemerkung. Ab $n = 16$ bzw. $s = 4$ braucht dies nicht mehr zuzutreffen, wie das Beispiel $p = 17$ mit $(\frac{2}{17})_4 = -1$ zeigt. Das Restsymbol in (A.12) ist dann notwendig.

Beweis von (1.10), (1.11) (*Stickelberger* [8])

Für $r, s \not\equiv 0(n)$ hat man nach (1.9)

$$G_r G_s = \sum_{\mu,\nu \in GF(p^f)} \chi^r(\mu)\, \chi^s(\nu)\, \xi^{S(\mu+\nu)}.$$

Die Glieder mit $\mu + \nu = 0$ liefern zu dieser Summe den Beitrag

$$\chi^r(-1) \sum_{\nu \in GF(p^f)} \chi^{r+s}(\nu).$$

Durch

$$\sigma = \mu + \nu \neq 0 \qquad \mu = -\sigma\tau, \qquad \nu = \sigma(1+\tau)$$

ist eine eineindeutige Zuordnung der Paare (μ, ν); $\mu, \nu, \mu + \nu \neq 0$ zu den Paaren (σ, τ); $\sigma \neq 0$, $\tau \neq 0, -1$ gegeben. Es folgt

$$\begin{aligned} G_r G_s - \chi^r(-1) \sum_{\nu \in GF(p^f)} \chi^{r+s}(\nu) &= \sum_{\substack{\sigma,\tau \in GF^*(p^f) \\ \tau \neq -1}} \chi^r(-\sigma\tau)\, \chi^s(\sigma(1+\tau))\, \xi^{S(\sigma)} \\ &= \sum_{\tau \in GF(p^f)} \chi^r(\tau)\, \chi^s(\tau+1) \sum_{\sigma \in GF(p^f)} \chi^r(-1)\, \chi^{r+s}(\sigma)\, \xi^{S(\sigma)} \\ &= \chi^r(-1)\, K_{r,s}\, G_{r+s}. \end{aligned}$$

Zusammen mit (1.6) und (1.10′) ergibt das

$$G_r G_s = \chi^r(-1) \cdot \begin{cases} p^f; & r+s \equiv 0(n) \\ K_{r,s} G_{r+s}; & r+s \not\equiv 0(n) \end{cases} \quad r, s \not\equiv 0(n). \qquad (A.13)$$

Beweis von (2.13′), (3.5)

Wegen $(v/p) = (-v/p)$; $p \equiv 1(4)$ gilt

$${}^pK_2 = \sum_{v \in \mathbb{Z}_p}{}' \left(\frac{v}{p}\right)_4 \left(\frac{v+1}{p}\right)_4 \equiv \left(\frac{(p-1)/2}{p}\right)_4 \left(\frac{(p+1)/2}{p}\right)_4 \equiv 1(2),$$

somit

$${}^pK_2 = a + \eta_4 b; \qquad (a, 2) = 1, \qquad (A.14)$$

$${}^pK_2^* = a + ib; \qquad (a, 2) = 1. \qquad (A.14^*)$$

Beweis von (2.17), (3.12′)

Zwei verschiedene rationale Primzahlen $p, q \equiv 1(8)$ zerfallen in $\mathbb{Q}(\sqrt{-2})$ wie folgt in Primfaktoren

$$p = \pi' \cdot \bar{\pi}' = A^2 + 2B^2, \ \pi' = A + B\sqrt{-2}; \qquad B \equiv 0(2),$$

$$q = \kappa' \bar{\kappa}' = C^2 + 2D^2, \quad \kappa' = C + D\sqrt{-2}; \qquad D \equiv 0(2).$$

Wir wollen die Reziprozitätsformel

$$\left(\frac{\pi'}{\kappa'}\right)_2 = \left(\frac{\kappa'}{\pi'}\right)_2 \qquad (A.15)$$

beweisen. Seien $\mathbb{Z}_p, \mathbb{Z}_q$ die Restklassenbereiche modulo π' bzw. modulo κ'. Dann gilt

$$\pi' = A + B\sqrt{-2} = 0 \in \mathbb{Z}_p \Rightarrow \sqrt{-2} = -\frac{A}{B} \in \mathbb{Z}_p,$$

$$\kappa' = C + D\sqrt{-2} = 0 \in \mathbb{Z}_q \Rightarrow \sqrt{-2} = -\frac{C}{D} \in \mathbb{Z}_q.$$

Damit können wir (A.15) rational, d.h. mit Legendresymbolen schreiben

$$\left(\frac{A - (C/D)B}{q}\right) \stackrel{?}{=} \left(\frac{C - (A/B)D}{p}\right). \qquad (A.15')$$

Ist $B = 2^\lambda B'$ mit ungeradem B', so haben wir mit $(2/p) = 1$ und dem Jacobi'schen Reziprozitätsgesetz

$$\left(\frac{B}{p}\right) = \left(\frac{B'}{p}\right) = \left(\frac{p}{B'}\right) = \left(\frac{A^2 + 2B^2}{B'}\right) = \left(\frac{A^2}{B'}\right) = 1,$$

also

$$\left(\frac{B}{p}\right) = \left(\frac{D}{q}\right) = 1; \qquad p, q \equiv 1(8). \tag{A.16}$$

Damit erhält (A.15′) bzw (A.15) die Form

$$\left(\frac{AD - BC}{pq}\right) \stackrel{?}{=} 1. \tag{A.15″}$$

Für $2^{\mu} \| (AD - BC)$ erhalten wir mit $(2/p) = (2/q) = 1$

$$\begin{aligned}\left(\frac{AD - BC}{pq}\right) &= \left(\frac{2^{-\mu}(AD - BC)}{pq}\right) = \left(\frac{(A^2 + 2B^2)(C^2 + 2D^2)}{2^{-\mu}(AD'' - BC)}\right) \\ &= \left(\frac{(AC + 2BD)^2 + 2(AD - BC)^2}{2^{-\mu}(AD - BC)}\right) \\ &= \left(\frac{(AC + 2BD)^2}{2^{-\mu}(AD - BC)}\right) = 1.\end{aligned}$$

Beweis von (3.11′)

Für $q = c^2 + d^2 \equiv 1(4)$; $c \equiv 1(2)$ gilt zunächst

$$\left(\frac{c}{q}\right) = \left(\frac{q}{c}\right) = \left(\frac{c^2 + d^2}{c}\right) = 1$$

und weiter

$$\left(\frac{2d}{q}\right) = \left(\frac{2cd}{q}\right) = \left(\frac{(c + d)^2}{q}\right) = 1,$$

$$\left(\frac{d}{q}\right) = \left(\frac{2}{q}\right); \qquad q \equiv 1(4). \tag{A.17}$$

LITERATUR

1. K. BURDE, Ein rationales biquadratisches Reziprozitätsgesetz, *J. Reine Angew. Math.* **235** (1969), 175–184.
2. K. BURDE, Sequenzen der Länge 2 von Restklassencharakteren, *J. Reine Angew. Math.* **272** (1975), 194–202.
3. K. BURDE, Zur Herleitung von Reziprozitätsgesetzen unter Benutzung von endlichen Körpern, *J. Reine Angew. Math.* **293/294** (1977), 418–427.
4. K. BURDE, Potenzen von Galoisfeldern, *J. Reine Angew. Math.* **307/308** (1979), 194–220.
5. G. EISENSTEIN, Einfacher Beweis und Verallgemeinerung des Fundamentaltheorems für die biquadratischen Reste, *J. Reine Angew. Math.* **28** (1844), 223–245.

6. E. HECKE, Vorlesungen über die Theorie der algebraischen Zahlen, New York, 1948.
7. H. v. LIENEN, Reelle Reziprozitätsgesetze für kubische und biquadratische Reste, *J. Reine Angew. Math.* **305** (1979), 140–154.
8. L. STICKELBERGER, Ueber eine Verallgemeinerung der Kreistheilung, *Math. Ann.* **37** (1890), 321–367.
9. K. S. WILLIAMS, A rational octic reciprocity law, *Pacific J. Math.* **63**, No. 2 (1976), 563–570.
10. K. S. WILLIAMS, Note on Burde's rational biquadratic reciprocity law, *Canad. Math. Bull.* **20**, No. 1 (1977), 145–146.
11. K. S. WILLIAMS, A rational sixteenth power reciprocity law, *Acta Arith.* **33** (1977), 365–377.